Information Technology Executive Council (ITEC)

ITEC Policy 7400A

Computer Security Awareness and Training Policy Requirements

Computer Security Awareness and Training Policy Requirements

Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

Minimum Requirements

Each Entity shall fulfill the following responsibilities:

1. Designate an individual who is responsible for all aspects of an Entity's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

Note: This responsibility should normally be part of the Information Security Officer's role.

2. Include any Entity-specific IT security training requirements in the Entity IT security awareness and training program.

Example: An Entity that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an IT security training program that addresses specific HIPAA data security requirements.

3. Require that all employees, contractors or other third parties receive IT security awareness training annually, or more often as necessary.

4. Provide additional role-based IT security training commensurate with the level of expertise required for those employees, contractors or other third parties who manage, administer, operate, and design IT systems, as practicable and necessary.

Example: Entity employees and contractors who are members of the Disaster Recovery Team or Incident Response Team require specialized training in these duties.

5. Implement processes to monitor and track attendance at IT security training.

6. Require IT security training as part of new employee orientation and thereafter on a yearly basis for the user to have) IT system users access rights to the Entity's IT systems, and in order to maintain these access rights.

7. Develop an IT security training program so that each IT system user is aware of and understands the following concepts:
    - Passwords including creation, changing, aging and the need to keep confidential.
    - Privacy and proper handling of sensitive information
    - Physical Security
    - Social Engineering
    - Identity theft avoidance and action
    - Email usage
    - Internet usage
    - Viruses and malware
    - Software usage, copyrights and file sharing
    - Portable devices
    - Proper use of encryption devices
    - Reporting
        a. Suspicious activity
        b. Abuse
8. Require documentation of IT system users' acceptance of the Entity's security policies after receiving IT security training